UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Seagate SATA hard disc drive, serial number 5VCEH45X, currently in secure evidence storage at the FBI, more fully described in Attachment A	)	Case No. 3:21-mc-1109

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Seagate SATA hard disc drive, serial number 5VCEH45X, currently in secure evidence storage at the FBI, more fully described in Attachment A

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B)	Transportation, Distribution, Receipt, and Possession of Child Pornography

The application is based on these facts:

See the attached affidavit of Special Agent Cassandra M. Sommers, Federal Bureau of Investigation.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Cassandra M. Sommers, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 5:13 p.m. *(specify reliable electronic means).*

Date: October 14, 2021

Youlee Yim You

Judge's signature

City and state: Portland, Oregon

Honorable Youlee Yim You, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Item to be Searched

The following digital device, which was turned over to the FBI by Daniel Midget on August 12, 2021, and is currently in secure evidence storage at the Federal Bureau of Investigation, 9109 NE Cascades Parkway, Portland Oregon 97220:

Seagate SATA hard disc drive, serial number 5VCEH45X

ATTACHMENT B

Data to be Seized

1. All data on the device described in Attachment A ("the device") that relate to violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B) (transportation, receipt, distribution, and possession of child pornography), including:

a. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, including digital images and video clips;

b. All images or video recordings that are self-produced and pertain to sexually explicit images of minors, or video recordings of minors that may assist in the location of minor victims of child exploitation or child abuse;

c. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or any attempt to commit any such offense;

d. Evidence of Internet usage for the transportation, receipt, distribution, or possession of child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage, IP addresses, and any screen names, usernames, email addresses, or passwords used to access the Internet or any accounts via the Internet;

e. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means

(including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

f. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

g. All records or information referring or pertaining to communications with others for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 U.S.C. § 2256, including chat logs, call logs, email communications, address books or contact list entries, and digital images sent or received;

h. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, such as images of minors depicted in underwear or partially undressed.

2. Physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the device or its data.

3. Passwords, password files, test keys, encryption codes, or other information necessary to access the device or its data.

4. Evidence of user attribution showing who owned or used the device at the time the things described in this attachment were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, items and articles of identification, documents, and browsing history.

5. Records evidencing the use of the Internet, including:

a. Records of IP addresses used;

b. Records of Internet activity, including caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered in any Internet search engine, and records of user-typed web addresses; and

c. Records of online data storage accounts and use of data storage accounts.

6. As used above, the terms "records" and "information" include all items of evidence in whatever form and by whatever means they were created or stored, including any form of computer or electronic storage and any photographic form.

Search Procedure

7. Because the device is already in law enforcement custody, it will be transported to a forensic laboratory for examination. The examination may require authorities to employ techniques, including computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection to determine whether it is evidence described by the warrant.

8. The initial examination of the device will be performed within a reasonable amount of time not to exceed 120 days from the date the warrant was executed. If the government needs additional time to conduct this review, it may seek an extension of time from the Court within the original 120-day period from the date the warrant was executed. The government shall complete this review within 180 days of the date the warrant was executed. If the government needs additional time to complete this review, it may seek an extension of time from the Court.

9. If, at the conclusion of the examination, law enforcement personnel determine that specific files or file folders on the device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without

authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

10. If an examination is conducted and it is determined that the device does not contain any data falling within the ambit of the warrant, the government will return the device to the owner within a reasonable period following the search and will seal any image of the device, absent further authorization from the Court.

11. The government may retain the device if it contains contraband or evidence, if it constitutes fruits or an instrumentality of a crime, or to commence forfeiture proceedings against the device or its data.

12. The government will retain a forensic image of the device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

STATE OF OREGON)
) ss: AFFIDAVIT OF CASSANDRA M. SOMMERS
County of Multnomah)

Affidavit in Support of an Application for a Search Warrant

I, Cassandra M. Sommers, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for approximately nine months. I am currently assigned to the FBI's Portland Field Office. As a federal law enforcement officer, I am authorized to investigate and make arrests for violations of federal law, and to apply for federal search warrants. I graduated from the FBI Academy at Quantico, Virginia, after completing a 19-week course of instruction. I have acquired knowledge and information about criminal conduct and investigation from many sources, including formal and informal training, other law enforcement officers, investigators, persons who I have interviewed, and my participation in investigations. I have investigated matters involving the sexual exploitation of children, including the online sexual exploitation of children, particularly as it relates to violations of Title 18, United States Code, Sections 2252A and 2422. As part of my duties as a federal agent, I work with local, state, and other federal agencies on joint investigations of federal offenses.

2. I submit this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a search warrant authorizing the search and examination of the following device, further described in Attachment A, for the items described in Attachment B:

a. Seagate SATA hard disc drive, serial number 5VCEH45X, which is presently in secure law enforcement custody at the Federal Bureau of Investigation, located at 9109 NW Cascades Parkway, Portland, Oregon 97220.

As set forth below, I have probable cause to believe that the items described in Attachment B constitute contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), which prohibit transporting, distributing, receiving, and possessing child pornography.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; a review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

Applicable Law

4. Title 18, U.S.C., § 2252A(a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography using any means or facility of interstate or foreign commerce, or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

5. "Child pornography" is defined in 18 U.S.C. § 2256(8), and includes any visual depiction of a child under the age of 18 years engaged in sexually explicit conduct. "Sexually explicit conduct" is defined under 18 U.S.C. § 2256(2) and includes sexual intercourse, whether genital-genital, oral-genital, anal-genital, or oral-anal; bestiality; masturbation; sadistic or masochistic abuse; and the lascivious exhibition of the genitals, anus, or pubic area of any person.

Background on Computers, Digital Devices, and Child Pornography

6. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have drastically changed how child pornography is produced and distributed.

7. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer by using a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer via a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

9. A computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years.

These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on one's person.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs and networks such as Gnutella and BitTorrent, among others. Collectors and distributors of child pornography also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

11. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that

were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

12. I know based on my training and experience and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

13. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices by using forensic tools. Indeed, the very nature of the electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

Background on Telegram

14. Telegram is an application that allows for encrypted communication between two parties anywhere in the world. The communication occurs over the Internet and is similar to traditional text messaging. Telegram allows either party to send text, emojis or emoticons, pictures, and videos. Telegram can be installed on any mobile device or computer and can be

accessed online via the Telegram website. It also has a built-in function allowing for "Secret Chat" wherein either party can set a certain timeframe for all messages to delete themselves from both sides of the conversation.

15. Based on my training and experience and on conversations I have had with others who investigate child exploitation offenses, I know that Telegram can be and has been used to trade and collect child pornography via links exchanged on the platform.

Statement of Probable Cause

16. On Saturday July 31, 2021, Daniel Midget called the FBI National Threat Operations Center and reported finding a hard drive containing child pornography on the ground outside of the Shilo Inn, located at 1506 NE 2nd Avenue, Portland, OR, 97232.

17. I interviewed Midget by telephone on August 10, 2021. Midget told me that on July 30, 2021, he was leaving the Shilo Inn at approximately 8:30 a.m. and saw a blue hard-shelled case laying on the ground near the trashcan. Midget opened the case and found three hard drives inside of it. Midget had previously purchased a hard drive reader for his business and used that device to view the contents of the three hard drives on his personal laptop computer.

18. Midget stated that he saw "explicit things" on one of the hard drives, which he described as "approximately 5-20 files of videos and 20-50 files were of children or bestiality." Midget stated that one of the folders contained a video of an adult male inserting his erect penis into the mouth of a prepubescent boy who was sitting on a bed.

19. Midget described a second video that depicted what he believed was "definitely" child pornography, stating "it was a video of an adult male walking up to a boy who was 5-10 years old." The child pulled the adult male's pants down and performed oral sex on him.

When asked why he thought the boy was a child, Midget noted that he did not have any pubic hair.

20. Midget viewed a folder on the hard drive that contained nude images of athletic teenage boys approximately 14-17 years old. There were no sex acts being performed in those photos. Another folder labeled "telegram" contained exports of media from an unknown person's Telegram page. Midget said he did not open the saved Telegram media files. Midget couldn't recall if there was a username associated with the files. I know from my training and experience, and from conversations I have had with other experienced law enforcement officers, that files saved from Telegram to the hard drive could lead to information identifying the hard drive's owner or user, as well as the Telegram account(s) that were involved in the media transfers.

21. Midget also said he viewed folders on the hard drive that contained documents such as property receipts, deconstructed ID cards, and other corporate documents with addresses leading back to the Rose Garden Shilo Inn. Midget suspected that the owner of the hard drive was using some of the documents, like the ID cards, for identity theft or identity fraud.

22. Midget advised me that he received unwanted and sometimes broken electronic items. He refurbished or repaired these items and then either sold them or kept them for his personal use. Occasionally Midget finds personal information on devices, such as bank information on laptops or cellular telephones that were donated to "Goodwill." Knowing some of this information could be used by criminals, Midget carefully safeguards and removes that content.

23. When Midget reviewed the three hard drives he found at the motel, he determined that two of them contained neither contraband nor any information identifying the previous

owner. The third drive contained the materials described above. Midget decided to keep the first two devices but recognized the need to report the offending material on the third device to the FBI.

24. At the end of the interview, Midget turned over the hard drive he suspected contained child pornography to investigators. The hard drive was placed in secure evidence storage at the Federal Bureau of Investigation offices located at 9109 NE Cascades Pkwy, Portland, OR, 97220, where it remains. The FBI has not examined or searched the hard drive. All of the data that was on the drive when Midget turned it over to the FBI is still on it now.

Search Procedure

25. In searching the device described above and in Attachment A, law enforcement personnel executing the search warrant will employ the following procedure:

a. Because the device is already in law enforcement custody, it will be transported to a forensic laboratory for examination. The examination may require authorities to employ techniques, including computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection to determine whether it is evidence described by the warrant.

b. The initial examination of the device will be performed within a reasonable amount of time not to exceed 120 days from the date the warrant was executed. If the government needs additional time to conduct this review, it may seek an extension of time from the Court within the original 120-day period from the date the warrant was executed. The government shall complete this review within 180 days of the date the warrant was executed. If the government needs additional time to complete this review, it may seek an extension of time from the Court.

c. If, at the conclusion of the examination, law enforcement personnel determine that specific files or file folders on the device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

d. If an examination is conducted and it is determined that the device does not contain any data falling within the ambit of the warrant, the government will return the device to the owner within a reasonable period following the search and will seal any image of the device, absent further authorization from the Court.

e. The government may retain the device if it contains contraband or evidence, if it constitutes fruits or an instrumentality of a crime, or to commence forfeiture proceedings against the device or its data.

f. The government will retain a forensic image of the device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Data to be Seized

26. To search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject

to the procedures set forth herein:

a. All data on the device described in Attachment A that relate to violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B) (transportation, receipt, distribution, and possession of child pornography), including:

(i) All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, including digital images and video clips;

(ii) All images or video recordings that are self-produced and pertain to sexually explicit images of minors, or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

(iii) All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or any attempt to commit any such offense;

(iv) Evidence of Internet usage for the transportation, receipt, distribution, or possession of child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage, IP addresses, and any screen names, usernames, email addresses, or passwords used to access the Internet or any accounts via the Internet;

(v) All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

(vi) All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

(vii) All records or information referring or pertaining to communications with others for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 U.S.C. § 2256, including chat logs, call logs, email communications, address books or contact list entries, and digital images sent or received;

(viii) All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256, such as images of minors depicted in underwear or partially undressed.

2. Physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the device or its data.

3. Passwords, password files, test keys, encryption codes, or other information necessary to access the device or its data.

4. Evidence of user attribution showing who owned or used the device at the time the things described in this attachment were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, items and articles of identification, documents, and browsing history.

5. Records evidencing use of the Internet, including:

a. Records of IP addresses used;

b. Records of Internet activity, including caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered in any Internet search engine, and records of user-typed web addresses; and

c. Records of online data storage accounts and use of data storage accounts.

6. As used above, the terms "records" and "information" include all items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

Retention of Image

27. The government will retain a forensic image of the electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

28. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that was seized, imaged, or examined.

Conclusion

29. Based on the foregoing, I have probable cause to believe that the device described above and in Attachment A contains contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1), (a)(2), and (a)(5)(B), as set forth in Attachment B. I

therefore request that the Court issue a warrant authorizing a search of the device described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

30. This affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Gary Sussman prior to being submitted to the Court. AUSA Sussman advised me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

(By telephone)
CASSANDRA M. SOMMERS
Special Agent
Federal Bureau of Investigation

Sworn via telephone at 5:13 p.m. on October 14, 2021, in accordance with Fed. R. Crim. P. 4.1.

Youlee Yim You
THE HONORABLE YOULEE YIM YOU
United States Magistrate Judge